The Double-Edged Sword of Health Data Breaches: A Comparison of Customer and Stock Price Perspectives on the Impact of Data Breaches of Response Strategies

Kristin Masuch
University of Goettingen
kristin.masuch@uni-goettingen.de

Maike Greve
University of Goettingen
maike.greve@uni-goettingen.de

Simon Trang
University of Goettingen
strang@uni-goettingen.de

Abstract

Unauthorized access to personal health data, known as data breaches, causes multi-faceted adverse effects and damage. Companies are trying to counteract the impact on customer relationships through recovery strategies such as compensation. On the other hand, there is also a negative effect on the company's stock price. Here, the literature suggests an opposite effect of response strategies, but this has not been explored further until recently.

Our study takes both perspectives into account and examines the impact of data breaches on the market valuation in the health sector through an event study. Our results show a controversial relationship: If companies offered compensation to their customers in response to a data breach, this had a negative effect on the company's stock price. Our paper discusses this finding and derives practical implications and lessons learned for response strategies in the case of recent data breaches in the health sector.

1. Introduction

The use of digital technologies, especially in the health sector, entails considerable benefits and substantial risks [1], [2]. These days, incidents of security breaches occur regularly, if not even daily [3], [4]. While on the one hand, protection against such attacks plays a significant role for businesses, companies also have to deal with the consequences of a security breach [5]. Due to the reporting requirements in many parts of the world, data breaches are very present and visible to customers [6]. This is particularly vital in the health sector, where sensitive personal data are involved [7]. Usually, this has severe consequences for customer loyalty and for the company's financial or market value.

Both aspects are addressed in current research. Studies have shown that data breaches directly impact the stock value and cause companies worldwide to lose billions of dollars [8], [9]. On the other hand, previous research addresses what measures companies can take to maintain customer loyalty and trust after such an incident. In this context, recovery actions such as compensation and apology are particularly promising strategies [10], [11]. These studies show that such recovery strategies are an impactful management tool to mitigate negative consequences after a data breach [11]

In complement to these two aspects, our study analyzes recent health data breaches regarding the impact on the company's stock value. Furthermore, we investigate the consequence of response strategies. The study aims to generate lessons learned and finding based on real response strategies used in practice. Therefore this research paper aims to answer the following research question:

RQ: *How do recovery strategies to customers in response to data breaches affect the stock value of companies in the health sector?*

In this study, we examined the impact of a data breach on the healthcare company's stock price. For this purpose, data breaches between 2007 and 2020 are identified and analyzed. The analysis is carried out using the methodology of the event study [22]. In addition to the general impact of data breaches on the stock price, we also investigate the temporal component's influence. Furthermore, we look at the effect of compensation as a selected recovery strategy. Again, we analyze whether the temporal aspect is important in connection with the recovery strategy. Our study complements research on health data breaches that have examined their financial impacts. We are the first who examine the effect of response strategies on market valuation in the health industry. In doing so, we uncover differential effects of companies' post-breach behavior and provide actionable guidance for practitioners.

The paper continues by discussing the related work that is relevant to our research. Firstly, we introduce previous research on health data breaches and the literature on the impact of data breaches on stock value.

URI: https://hdl.handle.net/10125/79842
978-0-9981331-5-7

Afterward, the data breach recovery literature is discussed, and the focus of this literature, namely compensation, is pointed out. Our paper continues by deriving three hypotheses that guide our analyzes, followed by a description of data collection. The event study's methodology is described, and the results are presented following the hypotheses. Lastly, the results are reflected on, and their implications for the literature and practice are discussed. Finally, this study's limitations and future research on this topic are mentioned, and the main conclusions are presented.

2. Related Work within Data Breach Research

2.1. Health Data Breaches and their Impact on the Stock Value

Previous research has shown that the effects of a data breach are reflected in the affected company's stock value. In general, it has been found that data breaches harm the stock value because they are adverse events that indicate that the company is being abused (e.g., [7], [20], [23]). Certain characteristics of data breaches and their effects have also been identified and investigated in previous studies. In this context, interactions with company characteristics and industries have also been identified [7], [20], [24].

One industry of specific relevance is the health sector. It contains highly sensitive personal health data and experiences public and political pressure to adopt new technological practices even if the surrounding infrastructure is not secured [1]. Regulations and public concerns emphasize this sector's sensitivity and pressure healthcare providers to secure patient data and comply with regulations [2]. However, research shows that the healthcare industry lags in security [13] and experiences security incidents like data breaches daily [3]. Even though this area is of such relevance, only limited research focuses on the financial harm of such security incidents

While research focusing on specific industries is limited, general security literature identified general findings on the impact of data breaches on the stock value. For example, Cavusoglu et al. [7] found that past data breaches had a weaker impact on stock price than current data breaches. In examining the effect of response strategies after a data breach, Gwebu et al. [21] show some initial path-breaking results. They state that under the premise that the data breach happened at a company with a low reputation, response actions included in the publication notice of the data breach show different effects on its stock value. Building on a taxonomy of crisis response strategy, Gwebu et al. [21] categorize the response strategies of companies after data breaches up to 2010 into four superordinate categories (accommodative strategy, moderate strategy, defensive strategy, image renewal) and finds that especially the image renewal and moderate response strategy have a significant positive impact on the stock value of companies with low reputation. The accommodative and defense strategy hypothesized a negative impact on the stock value; however, they could not confirm this. It is striking that many response actions are combined under one strategy and that the strategies are not clearly defined. The moderate strategy, for example, comprises two actions: ingratiation and justification. Whereby the ingratiation action in a data breach announcement positively influences the attitude of the stakeholders. However, justification addresses a completely different level. It is designed to minimize the severity of the data breach through statements. The accommodative strategy also combines two actions, the apology and the remedial actions. The strategy is said to combine positive and negative aspects when summarizing the actions. The apology and compensation, which fall under remedial actions, are perceived as an admission of guilt. In addition, the more strongly these are expressed, the more heavily the data breach is perceived. Otherwise, one could also assume in a positive sense that the company realizes the problem and will do something about it [21].

Overall, previous research informs our study on two main aspects. First, it can be stated that data breaches generally trigger a negative stock price, and the severity of the impact depends on various characteristics of the data breach. Features of particular interest in this context are the industry and the actuality of the data breach. Second, research to date informs that data breaches must be made public, forcing companies to get in touch with their customers, which often leads to a recovery strategy, which has a different impact on the stock price.

2.2. The Impact on Customer Behavior

Besides the risk that the data breach will affect the company's performance, immense damage can also be caused by the loss of customer loyalty [25]. Recovery strategies are often used to compensate for the loss of the customer [26], [27] for the breach of trust caused by a data breach. These strategies include information about the incident and actions taken by the company to restore the customer's confidence and stabilize the relationship with the company [16]. Research in the field of data breach recovery actions already includes a few studies that analyze the effect of company responses on customer behavior (e.g., [15], [16]). This literature evaluates which strategies can positively influence

customer behavior. In doing so, the studies generally focus on two main strategies, apology and compensation (e.g., [14], [16]).

While some aspects of apology are sometimes included the customers' notification after a breach, an especially complementary effective response action is to compensate affected customers [16]. In such cases, the customer is offered a monetary or non-monetary equivalent in the form of a product or service as compensation for the damage. Research has shown that compensation has a positive effect on customer attitudes, and thus adverse effects can be averted (e.g., [14]–[16]). Thus, it can be shown by this stream of research that the effect of response strategies from the customer perspective has already been investigated in recent years and that accommodative strategies, in particular, have a positive influence on customer behavior. However, it should be noted that the disclosure of a data breach is perceived and evaluated by the customers and investors of the affected company and that accommodative strategies are said to have a negative effect here, although not confirmed. Consequently, there is a lack of consideration of these additional receivers and conceptualization of the actual response strategies of companies in the event of a data breach and thus a comprehensive consideration that provides recommendations for management on how they should behave in this difficult situation.

3. Hypotheses development

Previous studies on data breaches and their impact on stock value can already provide some key insights and identify factors that influence stock value. It has been observed that data breaches generally harm stock prices because, as mentioned above, they are adverse events that indicate company abuse (e.g. [7], [20], [23], [24], [28]). Data breaches are publicly disclosed because as companies are obliged to inform those affected by a data breach. This often causes a negative reaction on those affected and on the stock market [5], [29].

Certain characteristics of data breaches could also be analyzed to examine their impact. Campbell et al. [18] noted in particular that security breaches in which the attacker gained access to confidential information damaged the stock value. Since the literature has shown that the health sector is one of the most common address sectors where data breaches occur [1], and we consider breaches that violate confidentiality [18], we make the following hypothesis:

H1: *Publicly announced health-related data breaches harm the stock value of the affected company.*

At the same time, it is becoming apparent that the security-critical data requested and stored by companies and the security risk for this data are continually increasing, especially given the background of growing digitization [30]. In recent years, there is a rising trend of initiatives to protect customers' privacy [31]. Initially, a few US states have passed laws obliging companies to notify their customers if their sensitive data has been compromised [24], [31]. As of today, 50 states have decided to pass such a law [10].

Recent findings also indicate that these current developments have immense financial consequences [32], which often also results in immense customer losses after a data breach, as customers become more aware of the security risk through the increased information [32], [33]. Therefore, we conclude that from the combination of the higher risk of attacks and the increasing awareness of data breaches, more recent data breaches show a more negative effect.

H2: *Health-related data breaches that have occurred in recent years have a stronger negative impact on stock market valuation than older breaches.*

Research has shown that various possible response strategies positively influence the behavior of customers after a data breach. The current literature focuses on the recovery actions, apology and compensation [15]. These theoretical constructs can also be found in reality. In particular, compensation can be found in various data breach response strategies in the health sector.

This response strategy is always positively presented in the literature and even works, from a theoretical perspective, in contrast to an apology in severe data breaches. In reality, the response strategies are not only perceived by customers but also by investors. Within this connection, various literature reports that the information given and the tone of the message influence the investors and thus the stock price. Here it is particularly important whether the message sounds positive or negative [34]–[36]. In case of a negative-sounding event, investors suspect losses on the part of the company and vice versa [37]. In offering compensation that is supposed to affect customer behavior positively, a negative tone is struck on the investor. A negative tone arises from the fact that much information is disclosed by offering compensation.

Furthermore, compensation affects investors as if it were a serious data breach that needs to be paid. In addition, compensation can have the same effect on investors as an admission of debt [38], [39]. We, therefore, formulate the following hypothesis:

H3: *Health-related data breaches for which the company compensates the affected have a negative impact on the company's stock value.*

4. Methodological Approach

The hypotheses are tested through an event study. Real data breaches from companies in the health sector, such as insurance and pharma, serve as a data basis. In general, the analysis focused on healthcare companies listed in the US, where data breaches occurred between 2007 and 2020. The following sections outline the data collection of the sample and the estimation design.

4.1. Data-Collection Procedure and Sample Selection

The data collected is secondary data related to 303 reports of data breaches by public U.S. companies. Among them, 71 companies are in the healthcare sector. Only listed companies (i.e., NYSE, AMEX, or NASDAQ) were included in the sample. First, company-specific data breach notifications were identified in the online database "Privacy Rights Clearinghouse" since 2007 [23], [40], [41]. Second, an online search was conducted to expand the database. As the costs of security breaches doubled between 2006 and 2007, 2007 was chosen as the starting year. A higher relevance of data breaches can be observed from 2007 on [42]. Between January 2007 and June 2020, more than 8000 reported data breaches were identified [43].

Based on this database, further sampling processes were carried out to identify the relevant data set. First, publicly known companies listed on the stock market at the time of the incident were identified. In addition, the companies had to be listed on the stock market during the estimated period, which was usually in the range of [130, 1] from the date of the incident. Subsequently, all identified data breaches were examined to determine whether they violated the data's confidentiality to represent only actual so-called data breaches in the sample [18], [44]. As a next step, each company's responses on the day of disclosure were researched in various media, such as on the company's respective websites and government databases. The data breaches, for which no information about the disclosure of the data breach was found, were removed from the study so that the final 71 data sets were included in the analysis.

Consequently, the following procedure was to collect the relevant stock data on the data breach. Since the literature does not provide a consensus on how long the estimation period for average yields should be before the event window, 130 days before the event is chosen in this study [45], [46]. The analysis itself is based on an event window consisting of one day before and one day after the official company statement [22], [45], [46]. If the date of the statement was a weekend or other non-trading day, the previous trading day was chosen as the event day. For the purpose of conducting the relevant market-adjusted event study, the closing price for each day of the estimation period is required for each undertaking. As a market reference for the estimation period, the closing price for the relevant market index, such as NYSE, NASDAQ, or SP500, is used. The stock data, and therefore the closing prices used in event analysis, are collected using Yahoo Finance's database of historical stock data [47].

Besides the information on the data breach events, the official announcements of the affected companies had to be collected. For this purpose, each company's official websites or the US Attorney General's Office databases were searched for press releases. If these were not available, news reports about the statement were used, quoting the official response and additional information about the violations. These news reports were searched using the Lexis-Nexis database and information from the Privacy Rights Clearinghouse database. In cases where no report of the incident was publicly available on the internet, the Wayback Machine's web archive was used (data collection period: 2020-11-01 to 2020-06-15). After collecting the data violation statements for each incident, they were encoded by two researchers. After several coding loops, different reaction strategies could be identified:

Table 1. Overview of the coded data set

Industry type	∑	Response strategy	Number of response strategies used
No health service	232	Comp. No Comp.	63 169
Fitness	3	Comp. No Comp.	0 0x Apology; 3x Whitewash; 0x No Response Strategy
Healthcare	43	Comp. No Comp.	27 3x Apology; 11x Whitewash; 5x No Response Strategy
Insurance	8	Comp. No Comp.	4 0x Apology; 4x Whitewash; 0x No Response Strategy
Pharma/Retail	17	Comp. No Comp.	3 2x Apology; 9x Whitewash; 3x No Response Strategy

Note: Response strategies are not necessarily used alone.

The inter-rater reliability in the coding of the categories, which was calculated using Cohen's Kappa, has an agreement of 0.6. However, the present work

initially focuses only on the recovery strategy by compensation for the reasons already explained.

4.2. Estimation Method

The event study methodology is chosen to investigate the effects of post-data breach announcements and response strategies. An event study is a statistical tool for measuring the impact of corporate events on stock value [20], which is regularly used for studies in the financial sector [22], [48]–[50]. The basic idea is that markets are efficient, and any information given to market participants directly impacts a company's stock value [45]. For example, investors are more positive about companies because of events that are likely to generate future profits and devalue companies when adverse events occur [37]. Several IS researchers are already using the event study methodology to determine the impact of IT-related events on each affected company [24]. This study will assess the impact of data breaches and the different response strategies associated with them on the value of the affected company.

This event study will be conducted using the standard approach, a market model event analysis. The expected normal returns are calculated based on the company's past stock performance in relation to the returns of the reference market in regression analysis [22]. The market model can be seen in Equation (1), where R_{it} is the return on the stock price of the i-th company for time t; R_{mt} is the total market return for time t and the market portfolio m; ε_{it} is the zero-average disturbance term and α_i, β_i are the parameters or slope of the market model [22].

$$(1)\ R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}$$

Based on the event study method's convention, we have the index return SP500 as the market return for our model. An estimated 120 days were determined, starting at t = 130 days before the event and ending at t = 11 days before the event. The date of the event is the day t = 0. As defined, data breaches are considered an attack in which data confidentiality has been compromised. Since these are events that only become public when the companies announce them, the date of the event, which is defined as time t=0, does not necessarily fall on the day of the actual attack but on the day of the announcement. Using the collected responses from companies [24], we have carefully selected the appropriate event date for each data breach contained in the data set.

The next step is to calculate the abnormal returns, AR, for company i on and around the event dates for the periods t=-1, t=0, and t=1. The abnormal returns are calculated using Equation (2), where AR is the abnormal returns, R is the normal returns, and $E(R_{it})$ is expected normal returns, as calculated in Equation (1) [45].

$$(2)\ AR = R - E(R_{it})$$

The cumulative abnormal returns are then calculated by Equation (3). Here the CAR is the cumulative abnormal returns of company i, AR is the abnormal returns, and t_1 and t_2 are the start and end dates of the event window [45]. In this case, an event window is selected that contains one day before the event date, the day of the event, and the following day, which gives t = (-1, 0, +1).

$$(3)\ CAR_i = \sum_{t_1}^{t_2} AR_{it}$$

The average CAR can be calculated for all companies in the sample using Equation (4). If the calculated CARs differ significantly from zero, an abnormal return due to the event is declared.

$$(4)\ CAR = \frac{1}{N}\sum_{j=1}^{N} CAR_i$$

5. Data Analysis and Results

The event study method provided CAR values for each data breach through Equation (3). Concerning the derived hypotheses, the mean value of the CAR was calculated for specific groups. All calculations are based on an [-1;1] event window to evaluate the stock value's short-term impact. As we only expect negative impacts of the CAR value, we conduct one-sided t-tests to validate that the mean value is statistically significantly smaller than zero.

As a first analytical step, we considered the full sample of 71 data breaches (see Table 1). For results show that for the event window [-1;1], the mean CAR is -0.0093 for all companies. This value can be interpreted that between one day before the public announcement of the data breach and one day after, the companies' stock value that is considered by the sample decreases on average by 0.93% compared compared to the average variance in stock value.

The hypothesis test shows that this figure is statistically significantly smaller than zero on the 5 level.

Table 2. Results using the full sample

Sample size	Mean CAR	t-value	p-value
71	-0.0093	-1.8762	**.0324****

*p<0.10; **p<0.05; ***p<0.01

The full sample was divided into two sub-samples by the year the data breach was announced publicly to investigate the effect of time. The first sub-sample considers data breaches between 2007 and 2010, while the second sub-sample includes data breaches from 2011 onwards. The sample is split in 2011 because the

previous literature examining data breaches and their response strategies only consider data breaches that happened before 2011, and new developments not yet considered can be identified starting in 2011 [21]. Table 2 shows that the more recent data breaches have a generally higher effect on the average CAR value. The average drop of 1.27% is statistically significantly smaller than zero on a 5% level. In contrast, data breaches before 2011 show an average drop in the stock value of 0.31%, which is not statistically significant.

Table 3. Results by event year

Year	Sample size	Mean CAR	t-value	p-value
<2011	25	-0.0031	-0.5616	.2898
>=2011	46	-0.0127	-1.8037	**.0389****

*p<0.10; **p<0.05; ***p<0.01

To analyze whether the response strategy influences the CAR value, we differentiate between data breaches, where the company offers compensation to its customers, and data breaches where customers did not receive any value. Separating by compensation offering shows that in 34 cases, almost half of the sample, the company offered a form of compensation. Such a reaction causes a statistically significant average drop of 1% on the companies' stock value. While the mean CAR value is also negative on average for the companies that did not respond with compensation, this mean value is not statistically significant. This shows that the response strategy harms the CAR value of the company.

Table 4. Results by response strategy

Response strategy	Sample size	Mean CAR	t-value	p-value
Comp.	34	-0.0100	-1.9068	**.0326****
No Comp.	37	-0.0088	-1.0571	.1487

*p<0.10; **p<0.05; ***p<0.01

By combining the sample split by year and by response strategy, the data shows that for data breaches before 2011, the CAR value even increased if companies did not offer compensation as a response strategy, while there is a slight decrease if compensation was offered. However, both results are not statistically significantly smaller than zero. In contrast, recent data breaches that occurred in 2011 or later have a negative statically impact if companies offered compensation on the stock value by an average of 1.17%.

While the decrease in stock value, if no compensation is offered, is not statistically significant. This result further emphasized that the negative effect of compensation on the stock value is a recent problem that increases in importance.

Table 5. Results by year and response

Year	Response strategy	Sample size	Mean CAR	t-value	p-value
<2011	Comp.	15	-0.0075	-1.1746	.1299
	No Comp.	10	0.00327	0.3083	.6176
>=2011	Comp.	19	-0.0117	-1.4863	**.0773***
	No Comp.	27	-0.0132	-1.2411	.1128

*p<0.10; **p<0.05; ***p<0.01

In summary, our results show that H1 can be supported, as the overall mean CAR for the total considered sample of health data breaches is statistically significantly smaller than zero. It can also be confirmed that data breaches that have happened recently have a more negative impact on a company's stock value (H2). Concerning the recovery strategy, we analyze the effect of compensation. The results show that offering compensation as a recovery negatively affects a company's stock value (H3). The effect is confirmed for recent data breaches.

6. Lessons Learned from Recent Health Data Breaches

As the analysis shows, data breaches in the health sector generally influence a company's stock value. Recent data breaches, in particular, have a negative impact on the stock value, so it can be assumed that the effects of data breaches will continue to increase in the future and will remain a relevant topic. Moreover, we examined the impact of compensation as a recovery strategy, since in about 50% of the health data breaches analyzed, compensation was used as a recovery strategy by the affected companies. Companies that are not in the healthcare sector, by contrast, use an apology in only 37% of data breaches. When the health company compensates its customers for the incident, a negative effect on its stock value is observed, which is particularly noticeable in recent incidents.

Thus, a negative, long-term effect of compensation on investor behavior can be suspected, and it is highly relevant to observe and learn from past data breaches. This result is controversial to previous research: The data breach response literature shows that compensation has a positive influence on the opinions and behavior of customers and may even have a long-term positive effect on customer loyalty [15], [16]. This contrasts with the reaction of investors who perceive compensation differently. For them, it appears to be an admission of guilt [35], [36], [39]. This prompts them to take a particularly negative view of the event.

It can be assumed that compensation indicates the severity of the damage so that investors expect a high business loss [34], [36]. However, the reality in terms of customer behavior shows precisely the opposite effect

[15], [16]. Therefore, it is particularly relevant for the affected company and the managers deciding on the strategies to consider both perspectives, the customer behavior, and the possible reaction of investors when planning the strategic disbursement of compensation to recover a data breach.

6.1. Practical Implications

The results obtained help companies in the healthcare industry rethink and optimize their response strategies for future response actions after similar data breaches. Previous research on response strategies for data breaches has shown that compensation after a data breach positively affects customer relations (e.g., [16]). It can thus be concluded that companies base their response strategies for a data breach primarily on restoring and strengthening the customer relationship since the loss of customer loyalty is one of the biggest problems after a data breach (e.g., [51]). It appears that health companies in particular often fail to take into account that their response strategies are read not only by customers, but also by investors. Indeed, unlike companies in other industries, they are much more likely to use a compensation.

Our study combines the choice of compensation as a recovery action by health companies with the impact on the stock price. Our results show that compensation following a health data breach has a more negative impact on companies' stock prices in the health sector than if the company does not offer compensation. This is controversial because the literature shows that compensation positively affects customer satisfaction [16]. Since this is the reason for the immense damage caused by a data breach, the company's compensation should actually be perceived positively by investors. However, investors are still trapped in their old patterns and feel that offering compensation is negative because the company may appear to admit its guilt and even make an implicit statement about the health data breach's severity [34]–[36]. Moreover, the fact that this is a particularly sensitive area of data, namely personal health-related data, is a further explanation for the negative behavior of investors.

Two points can be summarized; especially health companies should not only look at the customer perspective when choosing their response strategy but also consider what industry they are operating in and how investors might react to the combination of industry and response strategy. Investors should also rethink their behavior regarding how they react to a response strategy following a health data breach. As the literature has shown, compensation has a positive effect on customers' behavior and, therefore, on the company's value after a data breach, especially when the data is particularly sensitive, as in this case.

6.2 Contributions to Research

The present study complements the existing literature in three main areas.

Firstly, the literature can be supplemented in the area of security of companies in the health sector. While previous literature in this area focused on security strategies [2] in general, for example, predictive factors of healthcare data breach weaknesses [3], [4], our study extends the scope by focusing on the impact of data breaches on the stock value of a company. This area of research has been explored in the security literature so far (e.g., [23], [52]), but these studies do not differentiate by the operational industry or focus specifically on one specific industry sector. Indeed, our study also confirms the negative impact of data breaches on the stock price for companies in the health sector and generates the insight that recent data breaches are specifically investigated. In this context, the research of Yayla and Hu [24] and Cavusoglu et al. [7] is supplemented by the evidence that data breaches from 2011 onwards have a significant negative impact on a company's stock value in the health sector.

Second, the literature on data breach recovery actions will be complemented by a practical perspective on real-world data breach response strategies [16], [17]. It has been shown that the most commonly used recovery action compensation causes significant effects on stock prices.

Third, the present study combines the effect of compensation with the affected group. It is essential not to look at just one side of the situation. This is because previous research has only looked at either the investor or the customer perspective. However, it is clear from the study that when choosing compensation as a recovery strategy, both sides must be considered, as they have different impacts on the consequences of a company.

6.3. Limitations and Directions for Future Research

This study shows the initial results of the impact of data breaches in the health sector on the stock price of the company concerned. This study has some limitations but also offers opportunities for future research.

Since our study considers only compensation as a recovery action, it must be pointed out that this concentrated focus also leads to limitations. First, we can only identify compensations that are publicly known. So, if a company contacts the affected customers directly and offers them compensation, and

this is not publicly known, then it is not considered in our study. Secondly, we cannot guarantee that there are no other important aspects, such as the form of compensation or the wording of the message to the customer, that have an influence. At this point, future research could start and refine the distinction and analysis of recovery measures. Thirdly, the perception of investors was not investigated. It cannot be assumed how investors perceive the publications. Therefore, future research should examine how investors perceive the response strategies.

A further challenge arises from the chosen methodology. Our investigation considers the date of the public announcement of the data breach as the date of the event. Accordingly, the actual data violation has already taken place earlier, usually on a different day. This results in time distortion since in the period between the data breach and the publication of the data breach, information may already have been disclosed to the customers, or information may have been leaked to the public in some other way. This would distort the stock price on the day of disclosure because there may have been a negative impact on the company's value at an earlier uncontrolled and unknown time [24].

Lastly, this study aims to reveal the lessons learned from previous health data breaches. However, since we analyze companies' stock value, only those companies operating in the stock market are evaluated. This excludes many influencing operators of the health market. However, future research should also include such companies and address their data breach risk and how they should respond to data breaches. Hereby, the focus should not be limited to the recovery strategy compensation. For example, more cost-efficient strategies, such as apologizing, should also be considered.

7. Conclusion

This study deals with the effects of data breach response strategies in the health sector on the stock price of the affected companies. We examine 71 real health data breaches and their impact on the stock market price, considering the timing and the selected response strategy. An event study was used to analyze the heatlh data breaches that occurred between 2007 and 2020. We discover the controversy: Although the literature shows a positive effect on customer relationships, compensation has a negative impact on the company's value in the stock market. In addition, the study confirms that data breaches become more significant as they become more current, as seen in data breaches that occurred after 2011 damage the value of the stock. In summary, the study results add new insights to the existing literature since they address double-edged aspects of firm harm in the health sector and thus offer an opportunity for consistent, sector-specific practical application.

8. References

[1] C. M. Angst, E. S. Block, J. D'Arcy, and K. Kelley, "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly*, vol. 41, no. 3, Mar. 2017, pp. 893–916, doi: 10.25300/MISQ/2017/41.3.10.

[2] J. Kwon and M. Eric Johnson, "Health-care security strategies for data protection and regulatory compliance," *Journal of Management Information Systems*, vol. 30, no. 2, 2013, pp. 41–66, doi: 10.2753/MIS0742-1222300202.

[3] A. McLeod and D. Dolezel, "Understanding healthcare data breaches: Crafting security profiles," 2018.

[4] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decision Support Systems*, vol. 108, no. April, 2018, pp. 57–68, doi: 10.1016/j.dss.2018.02.007.

[5] P. Gaynor, "Data Security Breaches Pushing States into Action," *Knight Ridder Tribune Business News*, 2005.

[6] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack," *Computers & Security*, vol. 86, no. July, Sep. 2019, pp. 402–418, doi: 10.1016/j.cose.2019.07.001.

[7] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, 2004, pp. 70–104, doi: 10.1080/10864415.2004.11044320.

[8] M. E. Whitman, "In defense of the realm: Understanding the threats to information security," *International Journal of Information Management*, 2004, doi: 10.1016/j.ijinfomgt.2003.12.003.

[9] P. Dadhich, "Top 10 cybersecurity incidents in 2020," 2020. .

[10] NCSL, "Security Breach Notification Laws," 2020. .

[11] L. A. Gordon, M. P. Loeb, and L. Zhou, “The impact of information security breaches: Has there been a downward shift in costs?,” *Journal of Computer Security*, vol. 19, no. 1, Feb. 2011, pp. 33–56, doi: 10.3233/JCS-2009-0398.

[12] Ponemon Institute LLC, “2018 Cost of Data Breach Study: Impact of Business Continuity Management.,” 2018. .

[13] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, “Cybersecurity in healthcare: A systematic review of modern threats and trends,” *Technology and Health Care*, vol. 25, no. 1, 2017, pp. 1–10, doi: 10.3233/THC-161263.

[14] K. Masuch, M. Greve, and S. Trang, “Does It Meet My Expectations? Compensation and Remorse as Data Breach Recovery Actions-An Experimental Scenario Based Investigation,” 2019.

[15] M. Greve, K. Masuch, and S. Trang, “The More, the Better? Compensation and Remorse as Data Breach Recovery Actions – An Experimental Scenario-based Investigation,” in *WI2020 Zentrale Tracks*, GITO Verlag, 2020, pp. 1278–1293.

[16] S. Goode, H. Hoehle, V. Venkatesh, and S. A. Brown, “USER compensation as a data breach recovery action: An investigation of the sony playstation network breach,” *MIS Quarterly: Management Information Systems*, 2017, doi: 10.25300/MISQ/2017/41.3.03.

[17] T. Kude, H. Hoehle, and T. A. Sykes, “Big data breaches and customer compensation strategies,” *International Journal of Operations & Production Management*, vol. 37, no. 1, Jan. 2017, pp. 56–74, doi: 10.1108/IJOPM-03-2015-0156.

[18] K. Campbell, L. A. Gordon, M. P. Loeb, and L. Zhou, “The economic cost of publicly announced information security breaches: Empirical evidence from the stock market,” *Journal of Computer Security*, vol. 11, no. 3, 2003, pp. 431–448, doi: 10.3233/JCS-2003-11308.

[19] R. Kantsperger and W. H. Kunz, “Consumer trust in service companies: a multiple mediating analysis,” *Managing Service Quality: An International Journal*, vol. 20, no. 1, 2010, pp. 4–25, doi: 10.1108/09604521011011603.

[20] A. Garg, J. Curtis, and H. Halper, “Quantifying the financial impact of IT security breaches,” *Information Management and Computer Security*, vol. 11, no. 2/3, 2003, pp. 74–83, doi: 10.1108/09685220310468646.

[21] K. L. Gwebu, J. Wang, and L. Wang, “The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management,” *Journal of Management Information Systems*, vol. 35, no. 2, Apr. 2018, pp. 683–714, doi: 10.1080/07421222.2018.1451962.

[22] A. C. MacKinlay, “Event Studies in Economics and Finance,” *Journal of Economic Literature*, vol. 35, no. 1, 1997, pp. 13–39.

[23] K. M. Gatzlaff and K. A. McCullough, “The Effect of Data Breaches on Shareholder Wealth,” *Risk Management and Insurance Review*, vol. 13, no. 1, Mar. 2010, pp. 61–83, doi: 10.1111/j.1540-6296.2010.01178.x.

[24] A. A. Yayla and Q. Hu, “The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors,” *Journal of Information Technology*, vol. 26, no. 1, Mar. 2011, pp. 60–77, doi: 10.1057/jit.2010.4.

[25] Ponemon Institute LLC, “2013 Cost of Data Breach Study: Global Analysis.,” 2013. .

[26] P. R. Varadarajan, “From the Editor,” *Journal of the Academy of Marketing Science*, vol. 30, no. 4, Oct. 2002, pp. 285–285, doi: 10.1177/009207002236905.

[27] C. Grönroos, “New Competition in the Service Economy: The Five Rules of Service,” *International Journal of Operations & Production Management*, vol. 8, no. 3, Mar. 1988, pp. 9–19, doi: 10.1108/eb054821.

[28] M. L. Ettredge and V. J. Richardson, “Information Transfer among Internet Firms: The Case of Hacker Attacks,” *Journal of Information Systems*, vol. 17, no. 2, Sep. 2003, pp. 71–82, doi: 10.2308/jis.2003.17.2.71.

[29] I. Sherr and N. Wingfield, “Play by Play: Sony’s Struggles on Breach,” *Wall Street Journal*, 2011.

[30] G. Piccoli, J. Rodriguez, B. Palese, and M. Bartosiak, “The Dark Side of Digital Transformation: The case of Information Systems Education,” 2018.

[31] M. S. Gaynor and M. Z. Hydari, “I S P ATIENT D ATA B ETTER P ROTECTED IN C OMPETITIVE H EALTHCARE M ARKETS ?,” pp. 1–16.

[32] Ponemon, “Cost of Data Breach Study: Impact of Business Continuity Management,” 2018.

[33] S. Goel and H. A. Shawky, “Estimating the market impact of security breach

announcements on firm values," *Information & Management*, vol. 46, no. 7, Oct. 2009, pp. 404–410, doi: 10.1016/j.im.2009.06.005.

[34] E. Henry, "Are Investors Influenced By How Earnings Press Releases Are Written?," *Journal of Business Communication*, vol. 45, no. 4, Oct. 2008, pp. 363–407, doi: 10.1177/0021943608319388.

[35] S. P. Kothari, S. Shu, and P. D. Wysocki, "Do Managers Withhold Bad News?," *Journal of Accounting Research*, vol. 47, no. 1, Mar. 2009, pp. 241–276, doi: 10.1111/j.1475-679X.2008.00318.x.

[36] R. Telang and S. Wattal, "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price," *IEEE Transactions on Software Engineering*, vol. 33, no. 8, Aug. 2007, pp. 544–557, doi: 10.1109/TSE.2007.70712.

[37] E. F. Fama, "Efficient Capital Markets: A Review of Theory and Empirical Work," *The Journal of Finance*, vol. 25, no. 2, May 1970, p. 383, doi: 10.2307/2325486.

[38] R. Fehr and M. J. Gelfand, "When apologies work: How matching apology components to victims' self-construals facilitates forgiveness," *Organizational Behavior and Human Decision Processes*, vol. 113, no. 1, 2010, pp. 37–50, doi: 10.1016/j.obhdp.2010.04.002.

[39] M. J. Bitner, "Evaluating Service Encounters: The Effects of Physical Surroundings and Employee Responses," *Journal of Marketing*, vol. 54, no. 2, 1990, p. 69, doi: 10.2307/1251871.

[40] P. Rosati, M. Cummins, P. Deeney, F. Gogolin, L. van der Werff, and T. Lynn, "The effect of data breach announcements beyond the stock price: Empirical evidence on market activity," *International Review of Financial Analysis*, vol. 49, Jan. 2017, pp. 146–154, doi: 10.1016/j.irfa.2017.01.001.

[41] P. Rosati, P. Deeney, M. Cummins, L. van der Werff, and T. Lynn, "Social media and stock price reaction to data breach announcements: Evidence from US listed companies," *Research in International Business and Finance*, vol. 47, 2019, pp. 458–469, doi: 10.1016/j.ribaf.2018.09.007.

[42] R. Richardson, "CSI computer crime and security survey," 2008.

[43] Privacy Rights Clearinghouse, "Privacy Rights Clearinghouse," 2019. .

[44] M. Ko, K.-M. Osei-Bryson, and C. Dorantes, "Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms," *Information Resources Management Journal*, vol. 22, no. 2, Apr. 2009, pp. 1–21, doi: 10.4018/irmj.2009040101.

[45] Y. Konchitchki and D. E. O'Leary, "Event study methodologies in information systems research," *International Journal of Accounting Information Systems*, vol. 12, no. 2, Jun. 2011, pp. 99–115, doi: 10.1016/j.accinf.2011.01.002.

[46] G. Pettengill and J. Clark, "Estimating Expected Returns in an Event Study Framework: Evidence from the Dartboard Lumn," *Quarterly Journal of Business and Economics*, vol. 40, no. 3/4, 2001, pp. 3–21.

[47] Yahoo Finance, "Yahoo Finance Historical Stock Data Base.," 2019. https://de.finance.yahoo.com/ (accessed Oct. 20, 2019).

[48] J. J. Binder, "The event study methodology since 1969," *Review of Quantitative Finance and Accounting*, vol. 11, no. 2, 1998, pp. 111–137, doi: 10.1023/A:1008295500105.

[49] A. R. Cowan and A. M. A. Sergeant, "Trading frequency and event study test specification," *Journal of Banking and Finance*, vol. 20, no. 10, 1996, pp. 1731–1757, doi: 10.1016/S0378-4266(96)00021-0.

[50] D. H. Sandler and R. Sandler, "Multiple event studies in public finance and labor economics: A simulation study with applications," *Journal of Economic and Social Measurement*, vol. 39, no. 1–2, 2014, pp. 31–57, doi: 10.3233/JEM-140383.

[51] Ponemon Institute LLC, "2010 Annual Study: U.S. Cost of a Data Breach.," 2011. .

[52] A. Hovav, J. Han, and J. Kim, "Market Reaction to Security Breach Announcements," *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, vol. 48, no. 1, 2017, pp. 11–52, doi: 10.1145/3051473.3051476.

.